

Defense Intelligence Agency  
**Office of the Inspector General**



# Semiannual Report to Congress

April 1, 2020–September 30, 2020



Defense Intelligence Agency

## Office of the Inspector General

# Semiannual Report to Congress

3rd and 4th Quarters, FY 2020

### Additional Information and Copies

This report and the annex are posted on the Joint Worldwide Intelligence Communications System and on the Secret Internet Protocol Router Network. A copy of this report can also be found on the Internet at <https://oig.dia.mil/> and at <http://www.oversight.gov>.

To request physical copies of this report, contact the DIA Office of Inspector General at (202) 231-1010.

### Send us Your Audit and Inspection Suggestions

Defense Intelligence Agency

ATTN: Office of the Inspector General

7400 Pentagon

Washington, D.C. 20301-7400

**Are you aware of fraud, waste, or abuse  
in a DIA program?  
If so, report it!**

### DIA Inspector General Hotline

**Via phone**

(202) 231-1000

**Via email**

**NIPR:** [ig\\_hotline@dia.mil](mailto:ig_hotline@dia.mil)

# A Message From the Inspector General

It is with great pleasure that I present the Defense Intelligence Agency (DIA) Office of the Inspector General (OIG) semiannual report to the U.S. Congress covering the reporting period of April 1, 2020, through September 30, 2020.



Despite the challenges we encountered due to the COVID-19 pandemic, we executed meaningful and relevant work that aligns to our mission to promote economy and efficiency and detect and deter fraud, waste, and abuse. This period, we evaluated DIA's compliance with the Improper Payments Elimination and Recovery Act for Fiscal Year 2019. We determined the Agency was compliant and were able to issue a report without findings or recommendations. In addition, we audited DIA's IT service contracts and also audited how DIA manages its network and facility access for personnel who have departed the Agency. You can read more about these projects in our classified annex.

We also completed oversight work related to the Agency's information management and governance efforts. First, we evaluated DIA's oversight of special access programs, identifying numerous compliance shortfalls and issuing four recommendations to address these gaps. We also released a memorandum to DIA management that outlined our ongoing evaluation of its Foreign Disclosure Program and identified critical risks that required the Agency's immediate attention. Lastly, we decided to close our inspection of the Agency's electronic records management, determining there was significant overlap with the National Archives and Records Administration's efforts.

Furthermore, we published 13 investigative reports, of which 8 involved allegations of reprisal. We substantiated reprisal in one of the cases. We also substantiated allegations of time and labor fraud and misuse of Government resources, identifying a \$96,707 loss to the Government. Additionally, we investigated but did not substantiate allegations regarding fraud, unauthorized personnel actions, abuse of authority, and Privacy Act violations. Lastly, we issued 15 management referral reports.

Also worthy of highlighting is our new, fully operational Case Management and Tracking System. The system officially went live after this report period ending; however, this accomplishment was a significant feat worthy of sharing. Made possible by many of our staff members, the system provides our Investigative team with a warranted level of efficiency. However, our work does not stop there—we are now transferring legacy data from previously used databases and will be able to discontinue their use once complete.

Throughout this ever-changing time, one thing has remained the same—my team's unwavering dedication to the OIG mission. It is through their diligent work and steadfast spirit that our organization continues to compel management action and keep Congress fully and currently informed. Overall, they deeply recognize our duty to serve the Department of Defense, the Intelligence Community, and most importantly, the American people. I also thank the Director, DIA's senior leaders, and Congress for their continued support.



A handwritten signature in cursive script that reads "Kristi M. Waschull".

Kristi M. Waschull  
Inspector General

# Summary of Activities

## Reports and Recommendations

### Reports Issued



**Audits:** 3  
**Investigations:** 13  
**Inspections & Evaluations:** 3

### Recommendations



**Audits:** 25  
**Investigations:** 11  
**Inspections & Evaluations:** 29

## Potential Cost Savings



**\$8,458,936**  
 Questioned Costs



**\$5,182,720**  
 Unsupported Costs



**\$255,208,000**  
 Funds Put to Better Use

## Investigative Activity



**\$112,190**  
 Dollars Recovered

### Description

### Number

Cases Opened	9
Cases Closed	2
Referrals	15
Hotline Complaints	67

### Allegations

### Number of Cases

Privacy Act Violation	1
Reprisal	8
Time and Labor Fraud	4
Misuse of Government Resources	3
Intelligence Oversight	1
Employee Misconduct	1
Fraud	1
Abuse of Authority	2

## **Table of Contents**

---

<b>The DIA Office of the Inspector General.....</b>	<b>1</b>
<b>Office of the Inspector General Organization .....</b>	<b>2</b>
<b>Statutory Reporting.....</b>	<b>4</b>
<b>Summary of DIA Conference Reporting.....</b>	<b>5</b>
<b>Legislative and Regulatory Review .....</b>	<b>6</b>
<b>Appendix A. Statistical Tables.....</b>	<b>18</b>
<b>Appendix B. Index of Reporting Requirements.....</b>	<b>18</b>
<b>Summary of Audit Activity.....</b>	<b>7</b>
<b>Summary of Inspection and Evaluation Activity .....</b>	<b>8</b>
<b>Summary of Investigation Activity.....</b>	<b>9</b>
<b>Appendix B. Index of Reporting Requirements.....</b>	<b>22</b>
<b>Appendix C. Status of Recommendations .....</b>	<b>Annex<sup>1</sup></b>
<b>Appendix D. Audits, Inspections, Evaluations, and Investigations Closed Since April 1, 2020.....</b>	<b>Annex</b>

---

<sup>1</sup> The Annex contains caveated and classified information, and therefore provided under separate cover.



# The DIA Office of the Inspector General

---

The DIA Office of the Inspector General (OIG) is one of 75 Federal statutory Inspectors General (IGs) established by the IG Act of 1978, as amended. The IG Act contains OIG independence provisions, the objectivity of OIG work, and safeguards against efforts to impair objectivity or hinder OIG operations.

## Mission

Conduct independent, objective, and timely oversight across the Defense Intelligence Agency (DIA) Enterprise to promote economy; detect and deter fraud, waste, abuse, and mismanagement; and inform DIA and Congress. We accomplish this through independent audits, inspections, evaluations, investigations, and the OIG Hotline program.



## Vision

Foster an inclusive and dynamic team of professionals that is a catalyst for accountability and positive change, compelling a more unified, adaptive, relevant, and agile DIA Enterprise.

## Values

### Teamwork

Collaboratively partner internally and across organizational boundaries to achieve common goals.

### Integrity

Courageously adhere to the highest ethical principles and honor confidentiality, objectivity, and trustworthiness.

### Excellence

Provide the highest quality products and customer service.

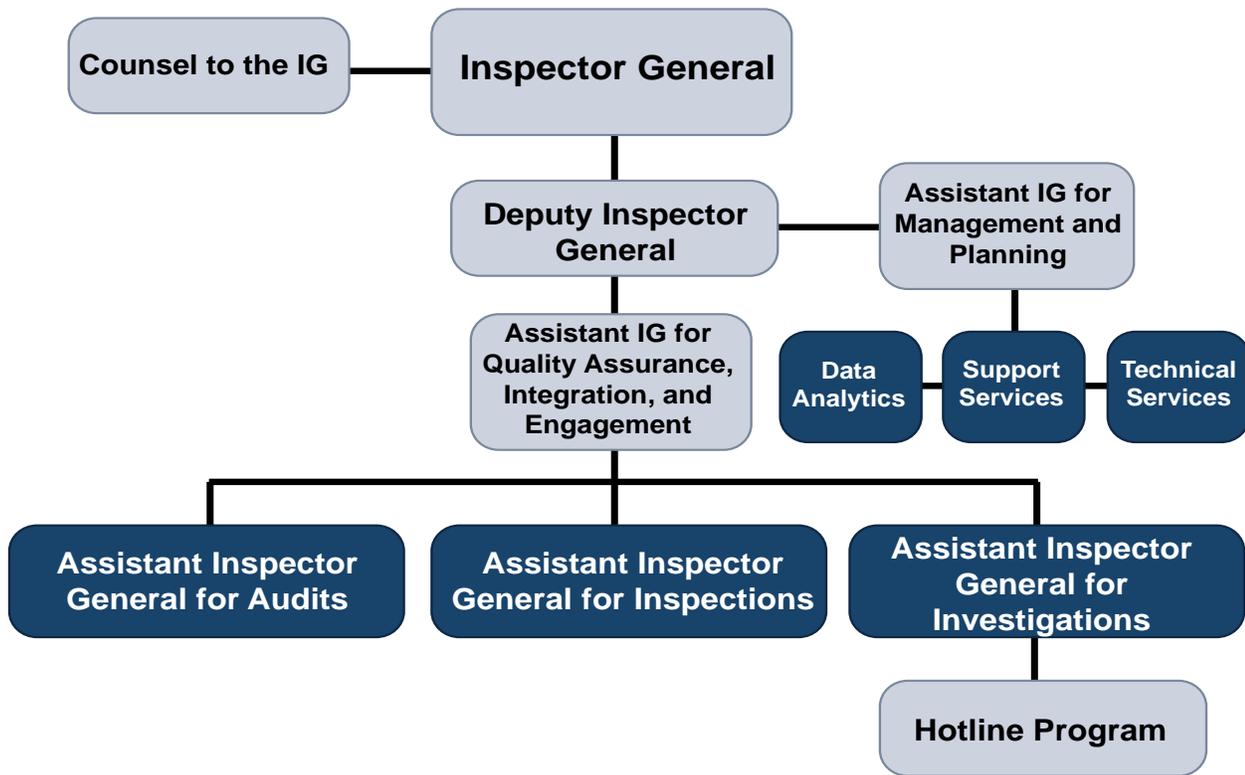
### Accountability

Steadfastly commit to deliver solutions that meet the highest standards.

### Initiative

Insightfully solve challenges and organize priorities.

# Office of the Inspector General Organization



## Audits

The Audits Division audits all aspects of DIA operations, providing recommendations that reduce costs; improve operational efficiency and effectiveness; strengthen internal controls; and achieve compliance with laws, regulations, and policy. It also conducts or oversees the annual independent audit of the Agency's financial statements

## Inspections and Evaluations

The Inspections and Evaluations Division evaluates the efficiency and effectiveness of DIA organizations, programs, and functions by conducting in-depth reviews across the Agency that examine and assess processes, procedures, internal controls, performance measures, compliance with regulatory and policy guidance, interrelationships, and customer satisfaction.



## Investigations

The Investigations Division conducts proactive and reactive administrative and criminal investigations. Its primary objectives are to detect, deter, and report fraud, waste, and abuse within DIA; develop sufficient evidence to successfully resolve all allegations and facilitate successful criminal prosecution or management-directed disciplinary action; and identify and report internal control weaknesses that could render DIA programs and systems vulnerable to exploitation. The Investigations Division, in coordination with the DIA Office of the General Counsel, also reports and investigates questionable intelligence activities, as defined by

Executive Order 12333, “United States Intelligence Activities,” as amended.

## **Hotline Program**

The Hotline Program is a confidential and reliable means for DIA employees and the public to report fraud, waste, mismanagement, and abuse of authority pertaining to DIA. The program’s primary role is to receive and evaluate concerns and complaints and determine the agency or responsible element best suited to take appropriate action.

## **Management and Planning**

The Management and Planning Division manages all administrative programs and services directly supporting OIG. The division enables useful audit, inspection, evaluation, and investigation activities and facilitates timely production of intelligence management and oversight products for DIA senior leadership and congressional overseers. Management and Planning Division functions include, but are not limited to, manpower, budget, records management, correspondence, Freedom of Information Act and Privacy Act, security, planning, training, information systems, and data analytics in support of the OIG mission.

# Statutory Reporting

---

## Reports to the Director of Refusal to Provide Information

Section 5(a)(5) of the IG Act of 1978 requires IGs to promptly report to the head of the establishment if information requested is unreasonably refused or not provided. No such reports were made during this reporting period.

## Reports Previously Issued That Lacked Management Comment Within 60 Days

Section 5(a)(10)(B) of the IG Act of 1978, as amended by the IG Empowerment Act, requires IGs to provide a summary of each audit, inspection, and evaluation report issued prior to the current reporting period for which no establishment comment was returned within 60 days of delivery of the report. No such reports were made during this reporting period.

## Significant Revised Management Decisions

Section 5(a)(11) of the IG Act of 1978 requires IGs to describe and explain the reasons for any significant revised management decisions made during the reporting period. We are not aware of revisions to any significant management decisions during this reporting period.

## Significant Management Decisions With Which the IG Disagrees

Section 5(a)(12) of the IG Act of 1978 requires IGs to provide information concerning any significant management decisions with which they disagree. During this reporting

period, there were no instances in which the IG disagreed with significant management decisions.

## Federal Financial Management Improvement Act of 1996

Section 5(a)(13) of the IG Act of 1978 requires IGs to provide information described under section 804(b) of the Federal Financial Management Improvement Act of 1996. This information involves the instances and reasons when an agency has not met target dates within its remediation plan to bring financial management systems into compliance with the law. In Fiscal Year (FY) 2018, DIA re-assessed its noncompliance with Federal financial management system requirements, and developed and implemented updated remediation plans to address areas of noncompliance. The Agency has not missed any of its remediation plan target dates.

## Attempts to Interfere With the IG's Independence

Section 5(a)(21) of the IG Act of 1978, as amended by the IG Empowerment Act, requires IGs to provide detailed descriptions of any attempts by their establishments to interfere with their independence. We did not experience any attempts to interfere with our office's independence during this reporting period.

## Public Disclosure

Section 5(a)(22) of the IG Act of 1978, as amended by the IG Empowerment Act, requires IGs to provide detailed descriptions of inspections, evaluations, audits, and investigations involving senior Government employees that were

closed during the reporting period without being publicly disclosed. Summaries of all such work are included in the appropriate sections of this report.

## Peer Reviews

Sections 5(a)(14–16) of the IG Act require IGs to report information about peer reviews that their offices have been subject to, including any recommendations that have not been fully implemented and a justification as to why. We were not subject to any peer reviews this reporting period. However, on November 6, 2017, the National Geospatial-Intelligence Agency OIG completed a peer review of our Inspections and Evaluations covering the preceding 3 years. All recommendations were implemented. Furthermore, on April 30, 2017, the Central Intelligence Agency completed a peer review of our Audits covering the preceding 3 years. We implemented all recommendations. We are currently conducting an audit peer review of the National Reconnaissance Office and will include the results in a future semiannual report (SAR).

## National Defense Authorization Act of FY 2020

Section 6718(b) of the National Defense Authorization Act of Fiscal Year 2020 requires IGs to report the number of investigations regarding unauthorized public disclosures of classified information to congressional intelligence committees, to include the number of reports opened, closed, and referred to the Attorney General for criminal investigation. We did not open, close, or refer any such investigations this reporting period.

# Summary of DIA Conference Reporting

Section 738 of the Consolidated Appropriations Act of 2019 requires the heads of executive branch organizations to provide certain details to the IG regarding the organization’s involvement in conferences. The table below represents reported conference costs with totals that exceed the reporting threshold of \$20,000. Most reported costs are estimates. We have not verified the accuracy or completeness of the data reported below; calculations are done by the appropriate Agency points of contact. We have also not verified whether DIA employees hosted or attended these conferences—either in person or virtually—in light of the COVID-19 pandemic.

Conference Name	Type	Estimated Cost	Actual Cost
DIA Activity Provider Conference	DIA-hosted	\$88,712	Pending
2020 American Copy Editors Society National Conference	Non-DoD-hosted	\$24,600	Pending
2020 Society for Technical Communications Summit	Non-DoD-hosted	\$22,050	Pending
2020 DoDIIS Worldwide Conference	DIA-hosted	\$830,944	Pending
<b>Total</b>		<b>\$966,306</b>	<b>-</b>



# Legislative and Regulatory Review

Section 4(a) of the IG Act of 1978 requires IGs to review existing and proposed legislation and regulations relating to the programs and operations of their respective organizations. Our reviews include legislation, executive orders, memorandums, directives, and other issuances. The primary purpose of our reviews is to assess the impact of proposed legislation or regulations on the economy and efficiency of programs and operations administered or financed by DIA, or the potential for fraud and abuse in these programs. During the reporting period, we reviewed proposed changes to the following:

Description	Number Reviewed
Legislation	15
Department of Defense Issuances	23
Defense Intelligence Agency Issuances	21
Office of the Director of National Intelligence Issuances	4
Executive Orders	4





### ***Audit of DIA's Information Technology Services Contracts, Project 2018-1006***

A summary of this audit can be found in the classified annex to this report.

### ***Audit of Controls for Managing Network and Facility Access for Separating Individuals, Project 2019-1003***

A summary of this audit can be found in the classified annex to this report.

### ***Evaluation of DIA's Compliance with the Improper Payments Elimination and Recovery Act for Fiscal Year 2019, Project 2020-1003***

We reviewed DIA's Financial Report and the documentation used to support its risk assessment for FY 2019 and determined that DIA complied with the Improper Payments Elimination and Recovery Act for FY 2019. DIA previously received relief from the Office of Management and Budget for reporting improper payments estimates and associated information, which we did not review as part of this project. Our final report was delayed due to the COVID-19 pandemic and was issued with no findings or recommendations.

### ***Other Audit Activity***

We closed 4 of the 29 recommendations open during this period<sup>2</sup> and continued to coordinate with Agency management on the status of its corrective action plans for the remaining recommendations. We are conducting fieldwork for projects related to Unplanned Price Changes and section 3610 of the Coronavirus Aid, Relief, and Economic Security Act. We also issued the draft report for the Evaluation of the Federal Information Security Modernization Act and target issuance of a final report at the end of October. Additionally, we are continuing our oversight of the audit of DIA's FY 2020 financial statements; the final report is due mid-November. We expect to report the results of these four projects in the next SAR.

---

<sup>2</sup> We closed 1 of the 14 recommendations listed in our last report, and 3 of the 15 new recommendations were issued during this period.



# Inspections & Evaluations

## ***Evaluation of DIA's Management of Special Access Programs, Project 2019-2007***

We evaluated DIA's oversight and administration of special access programs (SAPs), including the effectiveness with which the Special Access Program Central Office (SAPCO) governs DIA SAPs. We also assessed OIG identified special interest items. We concluded that DIA had limited oversight of SAPCO activities, and we found 13 compliance gaps in SAP administration. These issues impacted the Agency's ability to assure effective SAP governance. We issued 4 recommendations and made 14 suggestions to improve the problems identified. Management agreed with all recommendations and provided an action plan to implement them.

## ***Inspection of DIA's Electronic Records Management, Project 2020-2001***

We closed our electronic records management inspection and issued a closure memorandum due to significant overlap with the National Archives and Records Administration (NARA) inspection. In 2019, NARA completed a multi-agency inspection that included DIA. We assessed that continuation of the inspection would have been a duplication of effort. We did not issue any recommendations; however, our preliminary research and conclusions closely aligned with the deficiencies identified and recommendations made in NARA's report. Specifically, we noted areas where NARA also highlighted deficiencies in the areas of program management, records management, and oversight. In our closure memorandum, we stressed the importance of compliance with NARA's recommendations. We plan to follow-up with NARA to assess the need for future oversight.

## ***Memorandum to Management: Risk of Unauthorized Disclosures of National Security Information***

During our evaluation of DIA's Foreign Disclosure Program, we identified internal control issues regarding foreign disclosure and release decisions made in FY 2019. While our evaluation is ongoing, we issued a management memorandum because the issues we identified required immediate action to resolve. Specifically, we determined that some individuals making release decisions may not have satisfied the requirements outlined in IC, DoD, and DIA policies. This added unnecessary risk to DIA's foreign disclosure processes and may have negatively impacted foreign disclosure and release decisions. We issued three recommendations; management agreed with all recommendations and provided an action plan to resolve the identified issues. We plan to report the results in a future SAR upon completion of our evaluation.

## ***Other Inspection and Evaluation Activity***

We closed three recommendations and made seven new recommendations this reporting period. We continue to work with DIA management to close the remaining 29 open recommendations. We also terminated our strategic analysis evaluation due to issues with the scope and methodology of the assessment. We did not issue any findings or recommendations; however, we plan to initiate a follow-up evaluation on

this topic in the future. At the end of the reporting period, we issued a draft report of our evaluation of DIA's classification authorities and procedures and were awaiting management comments.<sup>3</sup> We also continue to work on our evaluations of the Foreign Disclosure Office, DIA's Management of the DoD All-Source Analyst Certification Program, and DIA's Management of Reserve Military Intelligence Capabilities. We plan to report these project's results in future SARs.

---

<sup>3</sup> This report has since been issued and will be reported in our next SAR.



## Investigative Activity Overview

### *Reprisal Investigations*

We completed eight investigations involving allegations of reprisal made during the previous reporting period.<sup>4</sup> We substantiated that reprisal occurred in one case.<sup>5</sup> We also determined that there was insufficient evidence to support the allegations of reprisal in six of the remaining seven cases. In the last case, we determined that the allegation did not meet at least one of the three elements of reprisal.<sup>6 7</sup>

During this reporting period, we received six reprisal complaints from DIA personnel: two of the complaints are presently under active investigation by our office, one complaint did not meet the elements of reprisal, and the remaining three complaints are presently under review.

When we determined that the aforementioned reprisal cases did not meet at least one of the three elements of reprisal, we notified the employee in writing of our determination. We also provided copies of each notification to the DoD IG and IC IG, for their awareness should an employee decide to appeal our determination.

### *Time and Labor Fraud and Misuse of Government Resources Investigations*

We investigated three cases involving time and labor fraud committed by three DIA employees. We substantiated all allegations and identified a \$96,706.87 loss to the Government. Additionally, in one of the cases, we substantiated allegations of misuse of Government resources. As all three cases represented a violation of Federal statute, we referred them to the appropriate Office of the Assistant U.S. Attorney, who declined to prosecute in all the cases. However, the DIA Office of the Chief Financial Officer is presently working to issue letters of indebtedness to recover the losses.

---

<sup>4</sup> A summary of these cases (2018-5071-OI, 2018-5072-OI, 2019-5010-OI, 2019-5026-OI, 2019-5040-OI, 2019-5052-OI, 2019-5055-OI, and 2019-5062-OI) can be found in the “Summaries of Published Investigative Reports” section in this report.

<sup>5</sup> A summary of Case 2018-5071-OI can be found in the “Summaries of Published Investigative Reports” section in this report.

<sup>6</sup> The three elements of reprisal are defined by Presidential Policy Directive 19 (PPD-19), “Protecting Whistleblowers with Access to Classified Information,” or by title 10, United States Code, section 1034 (10 U.S.C. § 1034), “Protected communication; prohibited of retaliatory personnel actions,” updated December 12, 2017, for civilian and military complainants, respectively.

<sup>7</sup> A summary of Case 2018-5072-OI can be found in the “Summaries of Published Investigative Reports” section in this report.

## ***Abuse of Authority Investigations***

We investigated one abuse of authority case involving three supervisory DIA employees, two of whom were DIA senior officials. This case involved two allegations—reprisal and abuse of authority.<sup>8</sup> In addition to determining that the case did not meet at least one of the three elements of reprisal, we also determined there was insufficient evidence that the supervisory employees abused their authority.



## ***Privacy Act Violation Investigation***

We investigated multiple allegations of Privacy Act violations made against two DIA senior officials, who were working at separate combatant commands (CCMDs). We determined that there was insufficient evidence to conclude that either senior official violated the Privacy Act.

## ***Fraud and Unauthorized Personnel Action Investigation***

We investigated allegations of fraud and unauthorized personnel actions made against a DIA military enlisted member. The allegation was made after the military member moved from Washington, DC, to Miami, Florida, without military orders. We determined there was insufficient evidence to conclude that the military member's actions were fraudulent or represented criminal intent. However, we did identify three management deficiencies that DIA management failed to follow Agency guidance for authorizing telework for Agency personnel. As a result, we issued three recommendations to DIA leadership and are awaiting a response.

---

<sup>8</sup> See previous footnote.

## Investigative Activities<sup>9</sup>

Description	Quantity
Cases Opened in Reporting Period	9
Cases Closed in Reporting Period	2
Cases Still Open at End of Reporting Period	43
Investigation Reports Issued in Reporting Period <sup>10</sup>	13
Referrals in Reporting Period (Number of Cases)	15
Referred to Management (Number of Cases) <sup>11</sup>	15
Referred to Prosecutorial Authority (Number of Cases)	3
Number of Persons Referred to Department of Justice for Criminal Prosecution	3
Number of Persons Referred to State or Local Prosecuting Authorities for Criminal Prosecution (includes military authorities)	0
Total Number of Indictments and Criminal Informations Resulting from Prior Referral to Prosecuting Authorities	0

---

<sup>9</sup> Description of Metrics: all metrics provided were developed as a result of reviewing relevant individual cases, including those opened and closed during this reporting period, and cases remaining open at the end of the previous reporting period (October 1, 2019–March 31, 2020).

<sup>10</sup> A summary of these cases can be found in the “Summaries of Published Investigative Reports” section of this report.

<sup>11</sup> A summary of cases 2018-5071-OI and 2020-5038-OI can be found in the “Summaries of Published Investigative Reports” section of this report.

## Summaries of Published Investigative Reports

### ***Reprisal, Case 2018-5071-OI***

We substantiated allegations of reprisal against two DIA military senior officials by a subordinate DIA military officer after the officer made protected communications to their senior leadership. We determined the officer was subject to retaliation after they reported counterintelligence violations and notified leadership of their intent to file a complaint with the DIA Equal Opportunity and Diversity Office. Specifically, we substantiated that the two military senior officials violated title 10, United States Code (U.S.C.), section 1034 (10 U.S.C. § 1034), “Protected communications; prohibition of retaliatory personnel actions” and DoD Directive 7050.06, “Military Whistleblower Protection,” April 7, 2015. We also determined that one of the two military senior officials made false official statements in violation of Article 107, Uniform Code of Military Justice, “False Official Statements”.

Both senior officials retired from active military service prior to the publication of our report of investigation. A copy of the report was forwarded to the Commanding General, Joint Force Headquarters, National Capital Region, for review and consideration of disciplinary action, as deemed appropriate. Currently, this case remains under review with the Commanding General’s office.

### ***Reprisal and Abuse of Authority, Case 2018-5072-OI***

We did not substantiate an allegation of reprisal made by a DIA employee against two supervisory DIA employees, including a DIA senior official. The employee alleged they received two significantly poor appraisals, without explanation, after they expressed concerns to management regarding their performance objectives. Additionally, the employee alleged that the two supervisory employees and a senior official bullied and harassed them. We determined that the personnel actions against the employee did not meet the elements of reprisal. Further, there was insufficient evidence to conclude that the supervisory DIA employees and senior official engaged in abuse of authority. However, we did identify a management deficiency that DIA management failed to follow Agency guidance for processing Joint Duty Assignment requests. As a result, we issued a recommendation to DIA leadership.

### ***Reprisal, Case 2019-5010-OI***

We did not substantiate allegations of reprisal made by a former DIA annuitant employee. The annuitant employee claimed they were subject to retaliatory acts by three supervisory DIA employees after making a protected communication to the DIA Office of Oversight and Compliance. Specifically, the employee alleged that their appointment was not renewed because they made the protected communication. The employee also stated that their FY 2018 performance appraisal was lower than any other rating they received as an annuitant. We subsequently determined that the actions taken by the supervisory employees were within management authority and DIA policy.

### ***Reprisal, Case 2019-5026-OI***

We did not substantiate an allegation of continued reprisal committed by two supervisory DIA senior officials against a DIA employee. However, we did determine that one of the senior officials abused their authority by requesting a review of the employee’s work to prevent the employee from returning to their former organization. The senior official who abused their authority retired from Federal service prior to the publication of our report of investigation. Of note, the employee and the senior official who retired were involved in a previous DIA OIG reprisal investigation.<sup>12</sup>

<sup>12</sup> A summary of Case 2017-5026-OI can be found in DIA OIG Semiannual Report to Congress (April 1, 2018–September 30, 2018) Main Report.

### ***Time and Labor Fraud, Case 2019-5032-OI***

We substantiated allegations of time and labor fraud, false official statements, false claims, and perjury by a DIA employee. The employee fraudulently prepared, signed, and submitted medical documentation from 2017 to 2019, and wrongfully received credit for claimed leave hours totaling 1,135.95 hours. We estimated a \$78,657.24 loss to the Government. Since this case represented a violation of law, we referred this case to the U.S. Attorney's Office for the District of Columbia, who declined to pursue criminal or civil prosecution. Recoupment of funds and disciplinary action are pending.

### ***Time and Labor Fraud and Misuse of Government Resources, Case 2019-5034-OI***

We substantiated allegations of time and labor fraud, false official statements, false claims, theft of Government funds, and misuse of Government resources against a DIA employee. We determined that the employee fraudulently prepared, signed, and submitted timesheets from May 13, 2018, to May 25, 2019, totaling 186.54 regular and overtime work hours that they did not work. We estimated a \$7,569.62 loss to the Government. As this represented a violation of law, we referred this case to the U.S. Attorney's Office of the District of Maryland (Southern Division) who declined to prosecute. Recoupment of funds and disciplinary action are pending.

### ***Reprisal, Case 2019-5040-OI***

We did not substantiate an allegation of reprisal made by a military enlisted member against a supervisory DIA employee. Specifically, the military member alleged that the supervisory employee provided unfavorable comments to the member's military rater about their work performance in retaliation for the member sharing concerns to leadership about comments the supervisory employee made, which the military member perceived as racist and unprofessional. Furthermore, the military member claimed that as a result they received an annual evaluation that included a "Not Ready Now" promotion recommendation. We determined that there was insufficient evidence to conclude that the supervisory DIA employee engaged in the prohibited personnel practice of reprisal, abuse of authority, or gross mismanagement. We found that the military member's annual evaluation was consistent with documented performance issues throughout their rating period, which occurred before the protected communication.

### ***Reprisal, Case 2019-5052-OI***

We did not substantiate an allegation made by a DIA employee who claimed they were subject to retaliation by five DIA supervisory employees, three of which were senior officials. The employee alleged that the supervisory employees retaliated against them after they reported security-related issues to the DIA Office of Security. The employee believed that they were treated disparagingly and unfairly, worked in a hostile environment, and was subjected to verbal abuse and threats for reporting the violations. We determined that there was insufficient evidence to conclude that any of the supervisory employees engaged in the prohibited personnel practice of reprisal, created a hostile work environment, or abused their authority.

### ***Reprisal, Case 2019-5055-OI***

We did not substantiate an allegation of reprisal made by a DIA contractor employee, who alleged that a supervisory DIA employee retaliated against them for making a protected communication to our office. Specifically, the contractor employee reported that their supervisor created a hostile work environment and misused Government information systems. The contractor employee alleged they were subsequently terminated without explanation. We determined there was insufficient evidence to conclude that the DIA

supervisory employee engaged in the prohibited personnel practice of reprisal, or otherwise engaged in retaliation, abuse of authority, or gross mismanagement. We also determined that the employee had not been terminated but agreed to be reassigned to an alternative work location in another DIA contractor position after remediation with their company. Furthermore, we investigated the contract employee’s claim that the supervisory employee misused Government information systems and committed time and labor fraud, and referred the allegation that they created a hostile work environment to the appropriate DIA leadership for review and action.<sup>13</sup>

### ***Reprisal, Case 2019-5062-OI***

We did not substantiate multiple allegations of reprisal made by a DIA employee, who alleged that a supervisory DIA senior official retaliated against them with a letter of counseling and a letter of reprimand for making a suggestion to their office leadership about an Agency work initiative. Upon further examination of the complaint, we could not determine whether the employee made a “protected communication.” We subsequently determined there was insufficient evidence to conclude that the DIA supervisory senior official engaged in reprisal, abused their authority, or harassed the employee.



<sup>13</sup> A summary of Case 2019-5034-OI can be found on page 14 of this report.

### ***Time and Labor Fraud, Case 2019-5065-OI***

We substantiated allegations of time and labor fraud, false official statements, false claims, and theft of Government funds against a DIA employee. We determined the employee signed and submitted fraudulent time and labor records between May 27, 2018, and June 22, 2019, totaling 110.13 regular hours that they did not work. Additionally, the employee claimed 18.34 compensatory hours and 29.31 credit hours that were unaccounted for. We estimated an \$8,627.43 loss to the Government. Since the case represented a violation of law, we referred it to the AUSA, who declined to prosecute. Disciplinary action against the employee is pending.

### ***Misuse of Government Resources, Case 2019-5066-OI***

We substantiated allegations of misuse of Government resources against a DIA senior official. The official used Government IT systems to complete work for their real estate business and to access sexually explicit and violent content while on official duty. We also determined the employee violated Agency policy that requires employees to report and obtain approval for outside employment. Disciplinary action is pending.

### ***Abuse of Authority and Misuse of Government Resources (Prohibited Personnel Practices), Case 2019-5069-OI***

We substantiated allegations of prohibited personnel practices and abuse of authority against a DIA senior official. We determined the senior official leveraged their position of authority and advocated for DIA to hire their family member. Further, we determined the senior official abused their authority and developed personal and business relationships for private gain by establishing an Agency outreach program that benefited that same family member's university and a private organization that the member led. Since this case represented a violation of law, we referred it to the AUSA, who declined to prosecute. Disciplinary action against the official is pending.

### ***Employee Misconduct, Case 2019-5077-OI***

We investigated allegations of misconduct against a DIA senior military official. Specifically, it was alleged that the military official made disparaging comments regarding sex, race, and sexual preference of U.S. Embassy personnel while in an official capacity. We determined the military official did not violate any provision of the Uniform Code of Military Justice, rule, or regulation; engage in any conflict of interest; or abuse their authority.

### ***Intelligence Oversight, Case 2019-5083-OI***

We did not substantiate an allegation that a DIA organization misused intelligence information to take an administrative action against a DIA employee. The organization suspended the employee's access because the employee was the subject of an investigation involving security matters. The organization was within its authority to suspend access while the investigation was ongoing.

### ***Privacy Act Violation, Case 2019-5063-OI***

We did not substantiate multiple allegations from a DIA employee, who alleged that two DIA senior officials assigned to two separate CCMD Directorates for Intelligence violated the Privacy Act by sharing the employee's security clearance information and security-related information with select CCMD personnel. We determined there was insufficient evidence to conclude that either senior official violated the Privacy Act.

## ***Fraud and Unauthorized Personnel Action, Case 2019-5064-OI***

We did not substantiate an allegation that a DIA military enlisted member committed fraud when they moved from Washington, DC, to Miami, FL without official orders. We determined there was insufficient evidence to conclude that the military member's actions were fraudulent or represented criminal intent. Furthermore, we determined that the military member moved at their personal expense, with no cost to the Government, and that the move served an official Government purpose. However, we also discovered an inconsistency in the accrual of their basic allowance for housing. Consequently, we made three recommendations to DIA leadership to address internal management control deficiencies identified during our investigation. DIA management is currently reviewing our recommendations.

## ***Time and Labor Fraud, Case 2020-5004-OI***

We substantiated an allegation of time and labor fraud, false official statements, false claims, and theft of Government funds against a DIA employee. We determined the employee fraudulently prepared, signed, and submitted timesheets from August 19, 2018, to August 31, 2019, claiming a total of 154.76 regular hours that they did not work. The total loss to the Government was estimated at \$10,480.01. As this was a violation of law, we referred this case to the U.S. Attorney's Office for the District of Columbia, who declined to pursue criminal or civil prosecution. Recoupment of funds and disciplinary action are pending.

## **Significant Management Referrals<sup>14</sup>**

### ***Review of Agency Speaker Engagement Vetting Processes, Case 2020-5038-OI***

We received two separate complaints regarding Agency plans to host a business executive speaker at a general professional development program for the workforce. Both complaints claimed that the speaker's political activist background and alleged partisan stance were inconsistent with the quality of presentations exhibited in the past. Further, both allegations expressed concern that scheduling the speaker at a Government agency and paying them with Federal funds potentially violated the Hatch Act.

During our review, we discovered that DIA management postponed the event because they did not properly vet the speaker and was not aware of the speaker's alleged partisan political stance. Further, we determined that there was insufficient evidence to support that DIA violated the Hatch Act. In addition, we referred this matter to Agency management and requested they review DIA's standard operating procedures for vetting organizations and guest speakers to ensure that appropriate controls are in place to avoid the appearance of Agency bias. A response from Agency management is pending.

## **Investigative Activity Support**

### ***Personnel Vetting***

This reporting period, we completed 3,054 checks for derogatory information within OIG records in response to 136 requests, which originated within DIA. These requests involved DIA military and civilians who are seeking job placement or advancement or are under consideration for awards.

---

<sup>14</sup> We define Significant Management Referrals as items that reflect a degradation in Agency policy and can potentially post Agency-wide impact. Referring such items provides transparency to the DIA workforce.

## Appendix A. Statistical Tables

**Table A-1: Audit and Inspection Reports With Questioned and Unsupported Costs**

Description	Number of Reports	Questioned Costs	Unsupported Costs
Reports for which no management decision was made by beginning of reporting period	3	\$8,458,936	\$5,182,720
Reports issued during reporting period	–	–	–
<b>Reports for which a management decision was made during reporting period</b>			
1. Dollar value of disallowed costs	–	–	–
2. Dollar value of allowed costs	2	\$7,926,508	\$4,650,292
Reports for which no management decision was made by the end of the reporting period <sup>15</sup>	1	\$532,428	\$532,428
Reports for which no management decision was made within 6 months	1	\$532,428	\$532,428

<sup>15</sup> Audit of DIA's Contract Surveillance, Project 2013-100010-OA: Published in DIA OIG Semiannual Report to Congress April 1, 2015–September 30, 2015. We found that DIA contracting officials and requiring activity personnel did not provide sufficient technical oversight to ensure that contractors performed in accordance with contract specifications. As a result, DIA had limited assurance that \$373.8 million in services and supplies met contract requirements. We also identified \$532,428 in unsupported costs for travel, tuition, and housing claimed under other direct costs in the invoices that were reviewed. At the end of the period, management sent us a memorandum requesting closure of this recommendation. We are reviewing it and will report the results of our review in the next SAR.

**Table A-2: Audit and Inspection Reports With Recommendations That Funds Be Put to Better Use**

Description	Number of Reports	Funds to be Put to Better Use
Reports for which no management decision was made by the beginning of reporting period	2	254,770,000
Reports issued during reporting period	1	438,000
<b>Reports for which a management decision was made during reporting period</b>		
1. Dollar value of recommendations agreed to by management	–	–
2. Dollar value of recommendations not agreed to by management	–	–
Reports for which no management decision was made by the end of the reporting period <sup>16 17 18</sup>	3	255,208,000
Reports for which no management decision was made within 6 months	2	254,770,000

**Table A-3: Investigations Dollar Recoveries in Reporting Period**

INVESTIGATION	CASE NUMBER	EFFECTIVE RECOVERY DATE	DOLLARS RECOVERED
Time and Labor Fraud and False Claims	2017-5089-OI	9 September 2020	\$103,607.85
Time and Labor Fraud and False Claims	2019-5065-OI	8 May 2020	\$8,582.03
<b>Total</b>			<b>\$112,189.88</b>

<sup>16</sup> Audit of Indefinite-Delivery/Indefinite-Quantity (IDIQ) Contracts, Project 2016-1004: Published in DIA OIG Semiannual Report to Congress April 1, 2017–September 30, 2017. We found that the Office of the Chief Financial Officer, Contracting Operations Division, could not determine the timeliness of IDIQ contract awards because it did not consistently establish contract milestones or record completion dates. As a result, DIA awarded six IDIQ contracts 3 to 5 months later than planned, and the delay for one contract increased the ceiling price by \$4.77 million. Management agreed with the corresponding recommendations.

<sup>17</sup> Audit of DIA’s Unliquidated Obligations, Project 2017-1006: Published in DIA OIG Semiannual Report to Congress April 1, 2018–September 30, 2018. We found that DIA was unlikely to spend about \$250 million of its FY 2017 appropriations, despite obligating nearly all funds. Management has closed three of the corresponding recommendations and is working on the remaining four open recommendations.

<sup>18</sup> Audit of IT Services Contracts, Project 2018-1006: Published in DIA OIG Semiannual Report to Congress April 1, 2020–September 30, 2020. We found that DIA did not properly administer award fees or monitor their effectiveness per regulation. As a result, more than \$438,000 in award fee payments could have been used for other mission requirements. Management agreed with the corresponding recommendation.

**Table A-4: Other Investigative Matters**

Description	Quantity
<b>Hotline Program</b>	
DIA OIG Hotline Inquiries Received in Reporting Period	67
DIA OIG Hotline Inquiries Closed in Reporting Period	53
<b>Intelligence Oversight</b>	
Cases Opened in Reporting Period	1
Cases Closed in Reporting Period	0
Cases Still Open at End of Reporting Period	2
Reports of Investigation Issued in Reporting Period	0
Referred to Management	0
<b>Management Referrals</b>	
Referrals in Reporting Period (external) <sup>19</sup>	1
Referrals in Reporting Period (DIA management) <sup>20</sup>	5

**Table A-5: Summary of Recommendations as of September 30, 2019<sup>21</sup>**

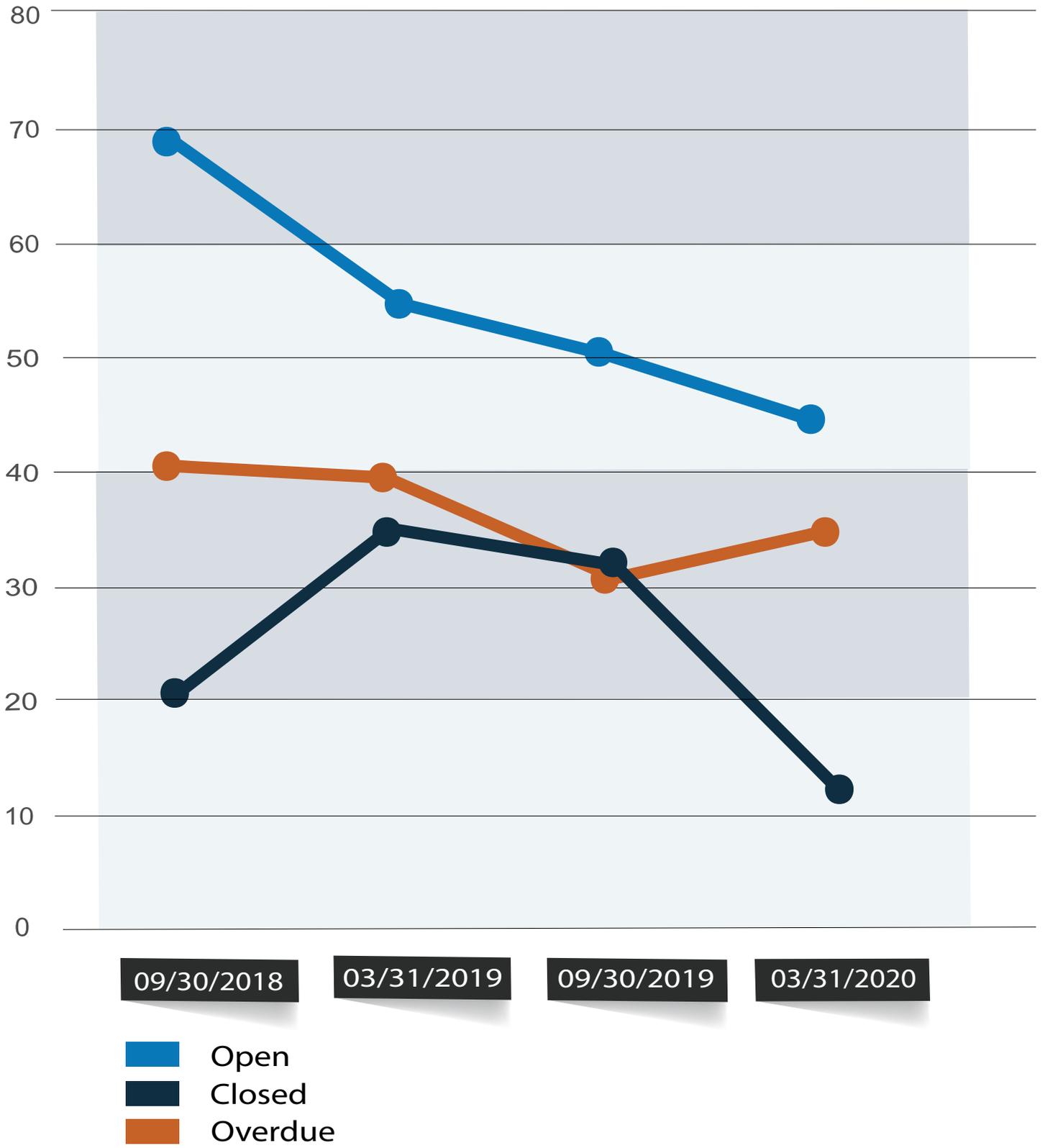
DESCRIPTION	QUANTITY
<b>Audits</b>	
Open Recommendations	25
Closed Recommendations	4
Overdue Recommendations	18
<b>Inspections</b>	
Open Recommendations	29
Closed Recommendations	3
Overdue Recommendations	23
<b>Investigations</b>	
Open Recommendations	11
Closed Recommendations	0
Overdue Recommendations	6

<sup>19</sup> A summary of Case 2020-5029-OI can be found in the classified annex of this report.

<sup>20</sup> Summaries of these cases can be found in the “Significant Management Referral” section of this report.

<sup>21</sup> “Overdue recommendations” refers to those recommendations that DIA management has not addressed within established

**Table A-6: Recommendation Trends**



# Appendix B. Index of Reporting Requirements

Semiannual Reporting Requirement		Page
4(a)(2)	<a href="#">Legislative and regulatory reviews</a>	6
5(a)(1)	<a href="#">Significant problems, abuses, and deficiencies</a>	7–17
5(a)(2–3)	Recommendations to correct significant problems, abuses, and deficiencies	Annex
5(a)(4)	<a href="#">Matters referred to prosecutive authorities and resulting prosecutions and convictions</a>	10–17
5(a)(5)	<a href="#">Reports to the Director, DIA of refusals to provide information</a>	4
5(a)(6)	<a href="#">List of reports issued during the reporting period</a>	7–17
5(a)(7)	<a href="#">Summaries of significant reports</a>	7–17
5(a)(8)	<a href="#">Statistical table showing questioned and unsupported costs</a>	18
5(a)(9)	<a href="#">Statistical tables showing recommendations that funds be put to better use</a>	19
5(a)(10)(A)	<a href="#">Summaries of reports previously issued that still lack management decision</a>	18-19
5(a)(10)(B)	<a href="#">Summaries of reports previously issued that lacked management comment within 60 days</a>	4
5(a)(10)(C)	Summaries of reports previously issued that have remaining unimplemented recommendations	Annex
5(a)(11)	<a href="#">Significant revised management decisions</a>	4
5(a)(12)	<a href="#">Significant management decisions with which the IG disagrees</a>	4
5(a)(13)	<a href="#">Federal Financial Management Improvement Act of 1996</a>	4
5(a) (14–16)	<a href="#">Peer reviews</a>	4
5(a) (17–18)	<a href="#">Investigations statistics and metrics</a>	12
5(a)(19)	<a href="#">Investigations involving substantiated allegations against senior officials</a>	10–17
5(a)(20)(A)	<a href="#">Descriptions of whistleblower retaliation</a>	10–17
5(a)(20)(B)	<a href="#">Establishment imposed consequences of whistleblower retaliation</a>	10–17
5(a)(20)(C)	<a href="#">Whistleblower retaliation settlement agreements</a>	10–17
5(a)(21)	<a href="#">Attempts to interfere with IG independence</a>	4
5(a)(22)	<a href="#">Public disclosure</a>	4
6718(b)	<a href="#">National Defense Authorization Act of FY 2020</a>	4



PCN 72001